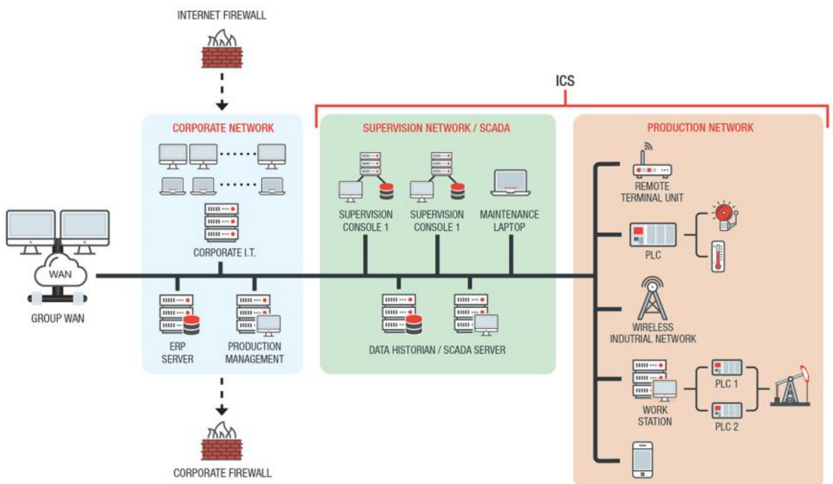
Use Case - Industrial Control

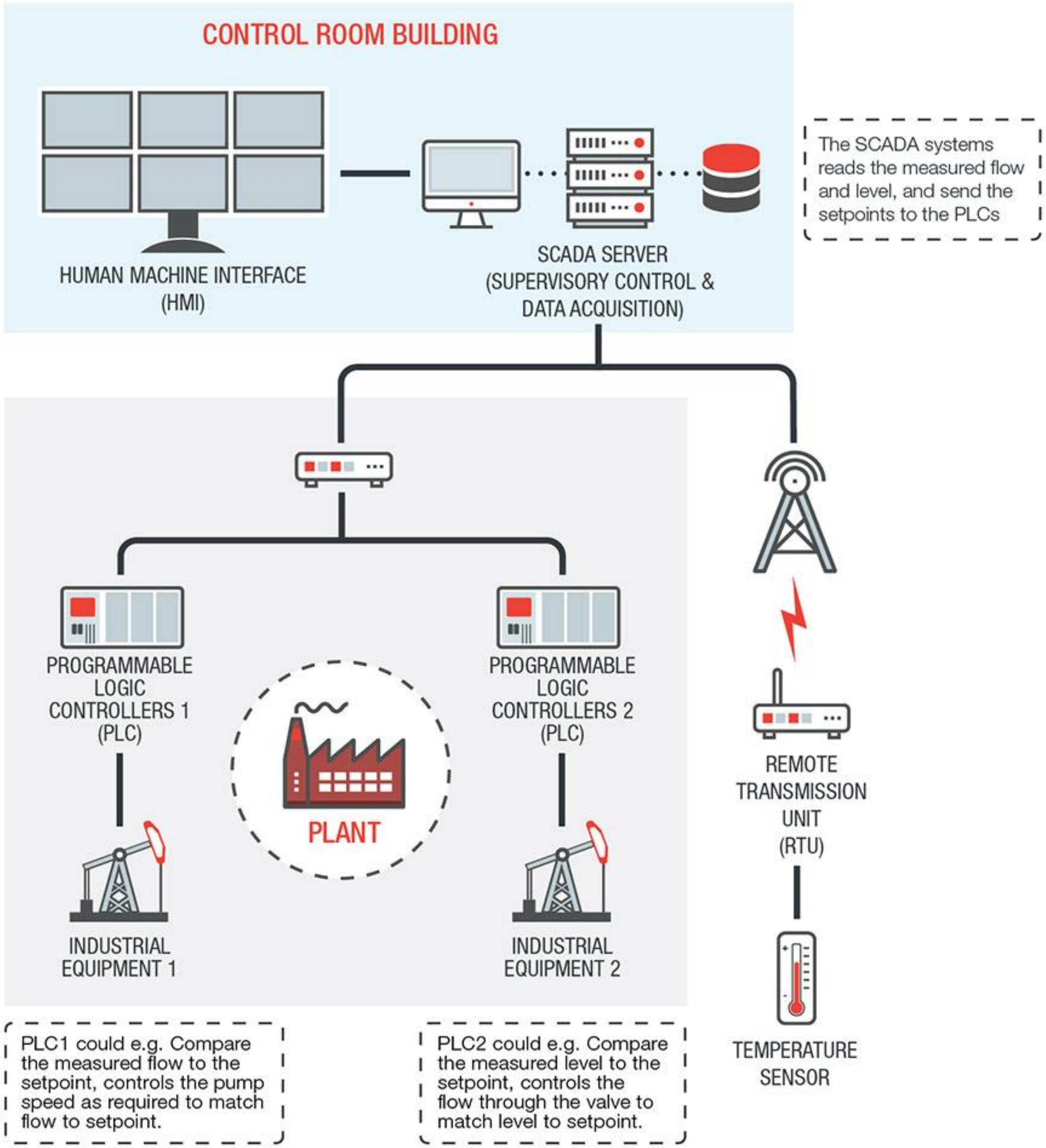
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control System (DCS)
- Components of an Industrial Control System (ICS) Environment:
  - IT and OT
  - Programmable Logic Controller (PLC)
  - Remote Terminal Unit (RTU)
  - Control Loop
  - Human Machine Interface (HMI)
  - Remote Diagnostics and Maintenance
  - Control Server
  - SCADA Server or Master Terminal Unit (MTU)
  - Intelligent Electronic Device (IED)
  - Data Historian

Industrial control system (ICS) is a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes. Depending on the industry, each ICS functions differently and are built to electronically manage tasks efficiently. Today the devices and protocols used in an ICS are used in nearly every industrial sector and critical infrastructure such as the manufacturing, transportation, energy, and water treatment industries.

There are several types of ICSs, the most common of which are Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS). Local operations are often controlled by so-called Field Devices that receive supervisory commands from remote stations.



What function does a SCADA system fulfill?



Communication within ICS Systems

Devices and control modules in ICS systems relay information through communication protocols. There are several communication protocols used through various ICS environments. Most of these protocols are designed for specific purposes such as process automation, building automation, power systems automation, and many more. These protocols were also developed to ensure interoperability between different manufacturers. However, there are some protocols that only work if the protocols and equipment come from the same manufacturer. The ICS protocols that are commonly found include:

Process Field Bus (PROFIBUS)

PROFIBUS uses RTU to MTU, MTU to MTU, and RTU to RTU communications in the field. There are two available variants: Profibus DP (decentralized peripherals), which is used to operate sensors and actuators through a central controller, and Profibus PA (process automation), which is used to monitor measuring equipment through a process control system.

Distributed Network Protocol (DNP3)

This is a protocol with three layers operating at the data link, application, and transport layers. This protocol is widely used in electricity and/or water and wastewater treatment plants.

Modbus

Since its introduction in 1979, the Modbus is considered one of the oldest ICS protocols. Modbus uses serial communications with the PLCs and has been the de facto communications protocol in an ICS environment. There are two types of Modbus implementations: Serial Modbus – which uses the high-level data link control (HDLC) standard for data transmission, and Modbus-TCP – which uses the TCP/IP protocol stack to transmit data.

Open Platform Communication (OPC)

The OPC is a series of standards and specifications for industrial communications. The OPC specification is based on technologies developed by Microsoft® for the Windows® operating system family (OLE, COM, and DCOM).

Building Automation and Control Networks (BACnet)

This is a communication protocol that is designed to control heating, ventilating, and air-conditioning control (HVAC); lighting; building access; and fire detection.

Common Industrial Protocol (CIP)

A CIP is a set of services and messages for control, security, synchronization, configuration, information, and so forth. The ICP can be integrated into Ethernet networks and the internet. CIP has a number of adaptations providing intercommunication and integration for different types of networks.

Ethernet for Control Automation Technology (EtherCAT)

An open-source communications protocol used to incorporate Ethernet into industrial environments. EtherCAT is used in automation applications with short updating cycles (≤ 100µs) and with jitter ≤ 1µs.

Common Threats to Industrial Control Systems

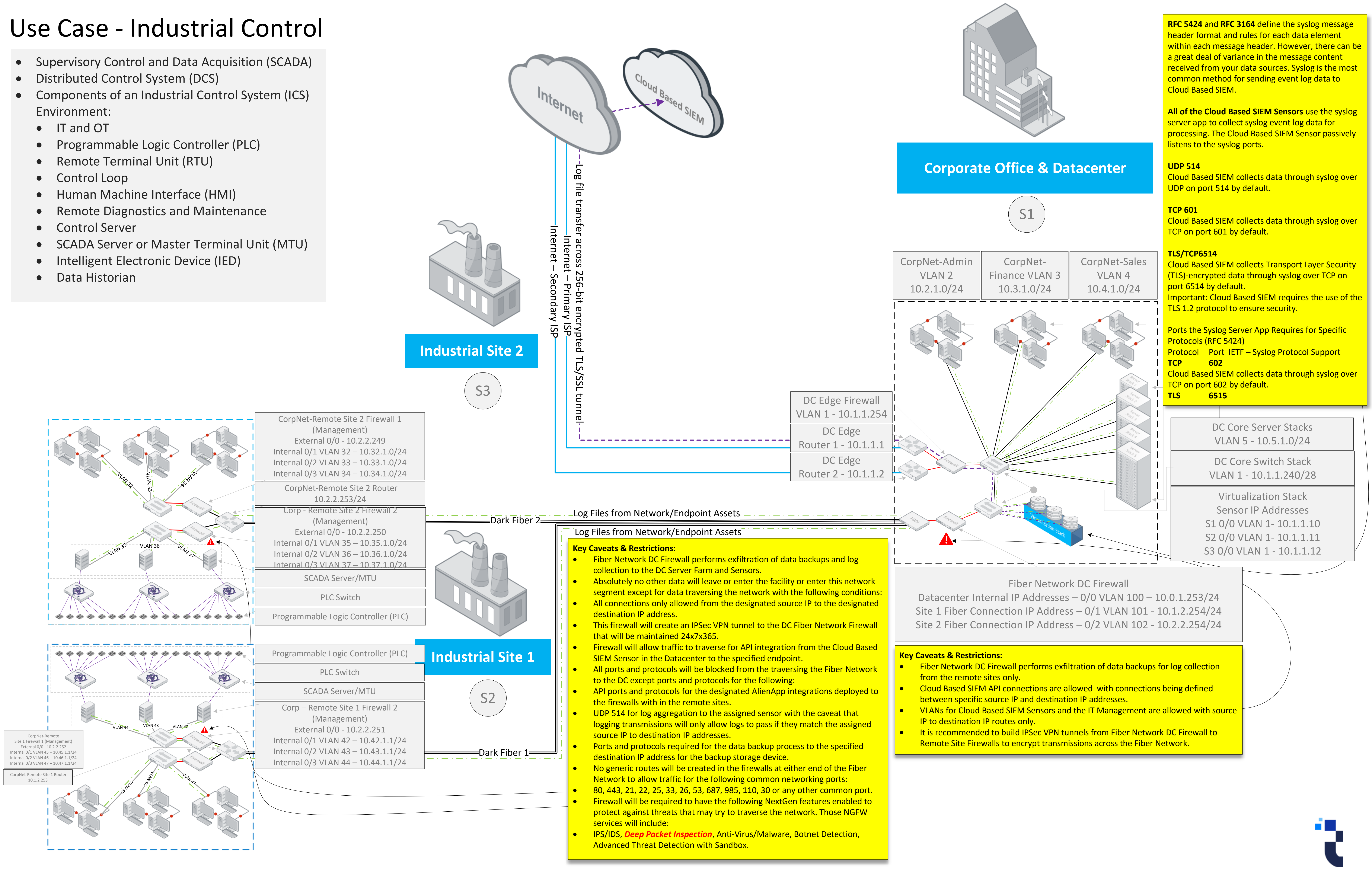
In order to improve system functions and productivity, every ICS constantly incorporates new technologies and software in both IT and OT. With IT and OT merged, they become bigger targets for cybercriminals. One of the common flaws of security solutions used in OT infrastructure is its inability to protect legacy control systems such as SCADA. In addition to that, organizations also have to face the rise of security challenges in new and emerging technologies, such as cloud computing, big data analytics, and the internet of things (IoT). Centralization introduces new and unknown vulnerabilities into the cyber ecosystem.

Attacks on ICS systems are often targeted attacks

Attacks on ICS systems are often targeted attacks that use the ICS entry path to gain a foothold inside a system which will allow them to laterally move into the organization. Among the most high-profile cases are the Stuxnet worm, which was used to manipulate centrifuges inside nuclear facilities in Iran, and BlackEnergy, which affected power generation facilities in Ukraine. Despite most of the attacks focusing on data theft and/or industrial espionage, both of the aforementioned cases demonstrated how malware had a kinetic effect. The Trend Micro whitepaper titled Cyber Threats to the Mining Industry explores how the mining industry is increasingly becoming a target of cyber espionage campaigns. These cyber espionage campaigns are designed to gain the latest technical knowledge and intelligence that will help some interest groups thrive and maintain competitive advantage.

Use Case - Industrial Control

- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control System (DCS)
- Components of an Industrial Control System (ICS) Environment:
  - IT and OT
  - Programmable Logic Controller (PLC)
  - Remote Terminal Unit (RTU)
  - Control Loop
  - Human Machine Interface (HMI)
  - Remote Diagnostics and Maintenance
  - Control Server
  - SCADA Server or Master Terminal Unit (MTU)
  - Intelligent Electronic Device (IED)
  - Data Historian



RFC 5424 and **RFC 3164** define the syslog message header format and rules for each data element within each message header. However, there can be a great deal of variance in the message content received from your data sources. Syslog is the most common method for sending event log data to Cloud Based SIEM.

All of the Cloud Based SIEM Sensors use the syslog server app to collect syslog event log data for processing. The Cloud Based SIEM Sensor passively listens to the syslog ports.

UDP 514
Cloud Based SIEM collects data through syslog over UDP on port 514 by default.

TCP 601
Cloud Based SIEM collects data through syslog over TCP on port 601 by default.

TLS/TCP6514
Cloud Based SIEM collects Transport Layer Security (TLS)-encrypted data through syslog over TCP on port 6514 by default.
Important: Cloud Based SIEM requires the use of the TLS 1.2 protocol to ensure security.

Ports the Syslog Server App Requires for Specific Protocols (RFC 5424)

Protocol	Port	IETF – Syslog Protocol Support
TCP	**602**	Cloud Based SIEM collects data through syslog over TCP on port 602 by default.
TLS	**6515**	

Key Caveats & Restrictions:

- Fiber Network DC Firewall performs exfiltration of data backups and log collection to the DC Server Farm and Sensors.
- Absolutely no other data will leave or enter the facility or enter this network segment except for data traversing the network with the following conditions:
- All connections only allowed from the designated source IP to the designated destination IP address.
- This firewall will create an IPSec VPN tunnel to the DC Fiber Network Firewall that will be maintained 24x7x365.
- Firewall will allow traffic to traverse for API integration from the Cloud Based SIEM Sensor in the Datacenter to the specified endpoint.
- All ports and protocols will be blocked from the traversing the Fiber Network to the DC except ports and protocols for the following:
- API ports and protocols for the designated AlienApp integrations deployed to the firewalls with in the remote sites.
- UDP 514 for log aggregation to the assigned sensor with the caveat that logging transmissions will only allow logs to pass if they match the assigned source IP to destination IP addresses.
- Ports and protocols required for the data backup process to the specified destination IP address for the backup storage device.
- No generic routes will be created in the firewalls at either end of the Fiber Network to allow traffic for the following common networking ports:
- 80, 443, 21, 22, 25, 53, 26, 53, 687, 985, 110, 30 or any other common port.
- Firewall will be required to have the following NextGen features enabled to protect against threats that may try to traverse the network. Those NGFW services will include:
- IPS/IDS, ***Deep Packet Inspection***, Anti-Virus/Malware, Botnet Detection, Advanced Threat Detection with Sandbox.

Key Caveats & Restrictions:

- Fiber Network DC Firewall performs exfiltration of data backups for log collection from the remote sites only.
- Cloud Based SIEM API connections are allowed with connections being defined between specific source IP and destination IP addresses.
- VLANs for Cloud Based SIEM Sensors and the IT Management are allowed with source IP to destination IP routes only.
- It is recommended to build IPSec VPN tunnels from Fiber Network DC Firewall to Remote Site Firewalls to encrypt transmissions across the Fiber Network.